Moves and/or changes

All relocations of microcomputer hardware must be requested through Network Services. Under no circumstances may any microcomputer hardware be removed or changed without authorization from Network Services.

Hardware inventory

Network Services maintains an inventory of every microcomputer the Company owns or leases. Each microcomputer is issued an asset number. A sticker showing the asset number is placed on each piece of hardware. This sticker must not be removed or modified by anyone outside Network Services.

FredMeyer

7.3 Purchasing Microcomputer Hardware/ Software

(5/96)

Statement

This policy provides Fred Meyer with the means to manage microcomputer hardware and software purchases throughout the Company. This type of management is necessary to:

- Help users select the right equipment and tools for the job
- Support the various software packages and hardware platforms
- Obtain appropriate budgetary authorization
- Maintain a current asset list of Company hardware and software

Scope

This policy applies to all Fred Meyer Stores employees.

Effective date

This policy is effective immediately and supersedes any previous policies.

Policy owner

Route all policy questions and suggested updates to the Network Services Manager.

Violation of this policy

Employees who violate this policy will be subject to disciplinary action up to and including termination.

Process overview

The following explains the process for requesting all hardware and software purchases. It is mandatory that all purchases of this type be approved by Information Services (IS).

Determine the need for the microcomputer hardware and/or software. ***If it is needed as part of an IS project,*** the request becomes part of the overall project—software and hardware costs become part of the system justification. ***If it is needed for a stand-alone microcomputer,*** follow the process below:

Stage	What Happens
1	Requestor (user) completes a *Project/Fixture Request* form (M1234) and obtains the signature of an assistant vice president or above.
2	Requestor submits request to Network Services.
3	Network Services project manager is assigned to review the request, make recommendation(s), and provide cost estimate(s).
4	Requestor and Network Services project manager select the best option and obtain approval from Network Services management team.
5	**If the request is approved,** Network Services purchases and installs hardware and/or software. **If the request is denied,** the requestor and Network Services project manager either try another option or further explain the business need and/or benefit of the request.

Guidelines for purchasing/leasing hardware or software

All microcomputer hardware and software purchases must be placed by Network Services.

Any hardware or software leases must be initiated by Network Services. Generally, leasing is not considered the most cost-effective solution.

Software installation and original disks

Anytime new software is purchased, Network Services installs it on the appropriate microcomputer. A backup copy of the software is then made for the user, and the original disk(s) are kept in a central software library. Do not attempt to install, remove, or copy (except for backup purposes) software from microcomputers without assistance from Network Services.

Moves and/or changes

All relocations of microcomputer hardware must be requested through Network Services. Under no circumstances may any microcomputer hardware be removed or changed without authorization from Network Services.

Hardware inventory

Network Services maintains an inventory of every microcomputer the Company owns or leases. Each microcomputer is issued an asset number. A sticker showing the asset number is placed on each piece of hardware. This sticker must not be removed or modified by anyone outside Network Services.

FredMeyer

7.4 Remote Access

(1/02)

Statement

Some employees need to be set up with remote access to Fred Meyer's data communications network. This policy outlines the procedures for setting up and terminating remote access to Fred Meyer Stores computer systems.

Remote access refers to electronic access from any location other than a Fred Meyer facility to a network access provider authorized by Fred Meyer.

Scope

This policy applies to all Fred Meyer Stores employees and contractors.

Effective Date

This policy is effective immediately and supersedes any previous policies.

Policy Owner

Route all policy questions and suggested updates to the Director of Fred Meyer Stores KTM Systems.

Violation of this Policy

Employees who violate this policy will be subject to disciplinary action up to and including termination.

Confidentiality and Security

It is important that those employees provided with remote access to the Company's communication network understand it is their responsibility to comply with corporate policies *4.1 Business Ethics* and *7.1 Information Security*. Managers should review both policies with all employees granted remote access.

Security is a shared responsibility. As such, It is important that management and all other employees, contractors, and vendors understand and comply with the guidelines regarding termination of user accounts outlined in this policy.

It is the responsibility of management (Fred Meyer, QFC, Smith's, Fry's, and Ralph's) to notify the Fred Meyer Office Systems Administration Group of any changes in status of employees, contractors, and vendors that use Fred Meyer Systems by submitting a SYS912 Security Request form. The form is available on the Office Systems Administration (OSA) site on FMinfo.

Eligibility

Before a manager submits a request for remote access, the employee must have the following:

- A proven need for access to the applications available through remote access
- Written approval from the department vice president
- The equipment required to support remote access, including IBM compatible personal computer capable of running the approved communication software
- A modem and telephone line

FredMeyer

Requesting Remote Access

The following table outlines the process to obtain remote access. Any problems should be directed to the Kroger West Support Center at (503) 233-4357. Managers should follow these steps to request that an employee be provided with remote access:

Stage	Who Does It	Action
1	Manager	**Requests from the Main Office:** ✦ Complete an SYS912 Security Request form, which can be obtained from the OSA website on FMinfo. ✦ Send the approved request to OSA through interoffice mail (04002/51N). **Requests from locations other than the Main Office:** ✦ Complete the form on the OSA website on FMinfo and send to: OSA at 04002/51N. ✦ Send the approved request to the default mailbox set up for that form.
2	IS	After receiving the request, OSA will approve or deny the request based on actual business need. ✦ If approved, OSA will send the employee: • A package containing a valid user ID and password, software for dial-up, instructions for setting up the software, a list of recommended equipment, and reference corporate policies: *7.1 Information Security* and *4.1 Business Ethics*. • ✦ If denied, the manager will be notified.
3	Manager	Have the employee install the necessary equipment and/or software within two weeks.

Terminating Remote Access

The following table outlines the process to terminate remote access.

Stage	Who Does It	Action
1	Employee	Contacts manager or department head if they know or think an employee and/or contractor has terminated employment with Fred Meyer.
2	Manager	Retrieves any Fred Meyer-supplied hardware and software from the terminated employee within three working days.
3	Manager	Submits a completed SYS912 Security Request form to Office Systems Administration at 04002/51N.
4	Manager	Ensures acknowledgment that the account has been disabled is obtained from Office Systems Administration via e-mail. **Note:** The manager may be required to produce proof that a request exists to disable the account and that the request has been completed. If the manager cannot provide this proof, (s)he will be held responsible for any breaches in security that occur as a result of not performing these required steps.

Note: If an employee is unable to contact management, or in extreme cases where an emergency (short notice) termination is required, contact Office Systems Administration at (503) 797-7458 (SPD 100, ext. 7458) immediately, and provide the Administrator with the name and user ID of the account that is to be disabled. You should leave a voice mail message and mark it urgent if you do not speak with an Administrator.

FredMeyer

7.5 Electronic Mail

(03/05)

Statement

The Fred Meyer electronic mail system (also known as *e-mail*) is intended for the exclusive use of authorized associates and contractors.

Lotus Notes is the e-mail system utilized by Fred Meyer to provide Fred Meyer associates and contractors with an efficient way to send and receive essential business information used to perform necessary job related duties and transactions.

Fred Meyer's e-mail system is a valuable business asset. The messages sent and received, like other documents created by associates in the course of a workday, are the property of Fred Meyer. This policy explains rules governing the appropriate use of e-mail and Fred Meyer's rights to access messages on the e-mail system.

Scope

This policy applies to all Fred Meyer associates.

Effective date

This policy is effective immediately and supersedes any previous policies.

Policy owner

Route all policy questions and suggested updates to the Fred Meyer Kroger Technology Manager (KTM).

Violation of this policy

Associates who violate this policy will be subject to disciplinary action up to and including termination. Associates using the e-mail system for defamatory, illegal, or fraudulent purposes and associates who break into unauthorized areas of Fred Meyer's computer system are also subject to civil liability and criminal prosecution.

Company rights

All e-mail communications are the property of the Company and are subject to review at any time, with or without notice, and are subject to corporate policy *7.1 Information Security.* Associates should not have any expectation of privacy with respect to messages or files sent, received, or stored on Fred Meyer's e-mail system. E-mail messages and files, like other types of Fred Meyer documents/correspondence, can be accessed and read by authorized management associates or authorized individuals outside the Company. However, ***before e-mail messages or files can be accessed, advanced authorization must be obtained*** from the Fred Meyer KTM; Group Vice President of Human Resources; or Vice President, Director of Loss Prevention (refer to corporate policy *7.1 Information Security*).

Internal use and access

E-mail can be an extremely useful business tool and is an effective way for associates to communicate with co-associates. By using e-mail, associates can decrease paperwork and the amount of time they spend on the telephone; however, e-mail should not be used to communicate sensitive or confidential information. Associates should anticipate that an e-mail message might be disclosed to or read by individuals other than the intended recipient(s), since messages can be easily forwarded to other individuals.

Managers should follow these steps to request access for associates with a business need for electronic communications:

Step	Action
1	✦ **For requests from store locations**, complete form SYS912 through FMinfo on the Store Home Page. Once the form is completed, click "Submit Request."
2	After receiving the request, IS will approve or deny the request based on actual business need. ✦ **If approved**, IS will provide the requesting manager with the associate's password. ✦ **If denied**, IS will contact the requesting manager.
3	Direct problems to the Kroger Support Center at SysSp 076.

External Use

Lotus Notes email is a business-use application only. It is not to be used for personal messages.

Store personnel are permitted to send e-mail outside of the Lotus Notes system only if it is for appropriate business use. Store Directors may contact Customers directly via e-mail when the Kroger Customer Care Center provides them with the Customer's e-mail information.

Prohibited uses of e-mail

Fred Meyer prohibits personal or private use of e-mail. Associates are strictly prohibited from using the e-mail system to do any of the following:

- Send or store offensive, obscene, or defamatory material, including racial or sexual slurs
- Engage in illegal, fraudulent, or malicious activities, including but not limited to sending or receiving documents in violation of copyright laws
- Annoy or harass other individuals, including but not limited to sending uninvited e-mail of a personal nature
- Send or store personal messages, chain letters, jokes, solicitations or offers to buy or sell goods, or other non-business material of a trivial or frivolous nature
- Engage in activities on behalf of organizations with no professional or business affiliation with Fred Meyer
- Participating in any newsgroup, mailing list, bulletin board, or other type of discussion forum that is not job-related
- Solicit outside business ventures or political or religious causes
- Conduct job searches outside Fred Meyer
- Gain unauthorized use to others' files, and/or to access systems restricted by government security laws or regulations
- Send, forward, or search non-business-related communications to gain unauthorized access to others' files
- Permit any unauthorized individual to access Fred Meyer's e-mail system
- Solicit unauthorized (by a senior vice president) donations or other non-profit activities

Passwords

Passwords are intended to keep unauthorized individuals from accessing messages stored on the system. For more information on passwords, refer to policy *7.1 Information Security*.

Storage

Storing large numbers of e-mail messages is discouraged. Storage of messages takes up large amounts of space on the server and can affect the system's performance. As a general rule, if a message does not require a specific action or response, it should be deleted after it is read. The system administrator will periodically purge mail older than 60 days.

Lotus Notes training

A Lotus Notes User's Guide is available and can be accessed from FMinfo.

Additional Lotus Notes training material may be obtained by contacting Information Systems at SysSp. 100 x3876 or by consulting the PC Training web page on FMinfo.

Questions

For questions, contact the Kroger Support Center by telephone at SysSp. 076. When prompted for a key phrase, say, "email."

FredMeyer

7.6 PC Backups & Off-Site Storage

(11/97)

Background

Ensuring the protection of vital data through periodic backups is essential for effective business continuity. Backing up vital data and storing these backups at an off-site facility is an important part of the Company's disaster recovery plan.

Mainframe, mid-range, and LAN server computer files are required to be backed up on a regular basis and stored off-site. This allows for disaster and file integrity recovery based on the requirements established by the responsible department manager.

Statement

Information Services requires that employees using personal computers backup critical business information stored on their personal computer on a regular basis.

Critical business information and backup frequency should be determined by the department manager based on how frequently the information is used to make business decisions and/or how easily the information would be to reproduced. Managers should contact Network Services to discuss the most effective method to perform regular backups. Each department manager is responsible for ensuring that critical business information is backed up a regular basis.

Non-critical business information stored or used on a personal computer is the responsibility of the employee using that personal computer.

Scope

This policy applies to Fred Meyer Stores employees.

Effective date

This policy is effective immediately and supersedes any previous policies.

Policy owner

Route all policy questions and suggested updates to Chief Information Officer.